SECRET INFORMATION STORAGE DEVICE

Patent number: JP2000029792
Publication date: 2000-01-28

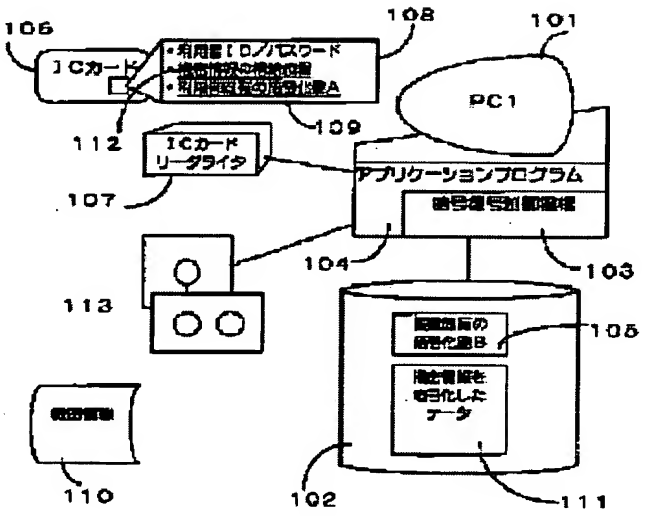
Inventor: TOMIZAWA SATOSHI
Applicant: HITACHI LTD

Classification:
- international: ***G06F12/14;*** **G06F12/14;** (IPC1-7): G06F12/14
- european:
Application number: JP19980195353 19980710
Priority number(s): JP19980195353 19980710

Report a data error here

Abstract of **JP2000029792**

PROBLEM TO BE SOLVED: To improve the confidentiality by storing information on a user, information showing the storage destination of secret information, and an encoding key characteristic of the user on a small-capacity medium and generating and storing a key characteristic of the device on a hard disk. SOLUTION: At incorporating, a key B105 characteristic of the device is generated and stored on an external storage device 102. Then the user actuates an encoding control mechanism 103 to register information 108 on the user. The contents of the information 108 of the user consist of a user ID, a password, and the encoding key A109 characteristic of the user. Then the user specifies desired secret information 110 to be concealed. An encoding control mechanism 103 reads the secret information 110 out and encodes it with a key A109 characteristic of the user. Consequently, a file obtained by further encoding the obtained file with the encoding key 105 characteristic of the device is written to a location such that the user specifies on the external storage device of the device. The location that the user specifies is written as a storage location 112 of the confidential information to an IC card 106.



Data supplied from the ***esp@cenet*** database - Worldwide

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-29792

(P2000-29792A)

(43) 公開日 平成12年1月28日(2000.1.28)

(51)Int.Cl.[7]	識別記号	F I			テーマコード(参考)
G06F 12/14	320	G06F	12/14	320 C	5B017

審査請求 未請求 請求項の数 3 OL (全 8 頁)

(21) 出願番号 特願平10-195353

(22) 出願日 平成10年7月10日(1998.7.10)

(71) 出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72) 発明者 富澤 智
神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所情報システム事業部内

(74) 代理人 100068504
弁理士 小川 勝男

Fターム(参考) 5B017 AA06 BA05 BA07 CA14

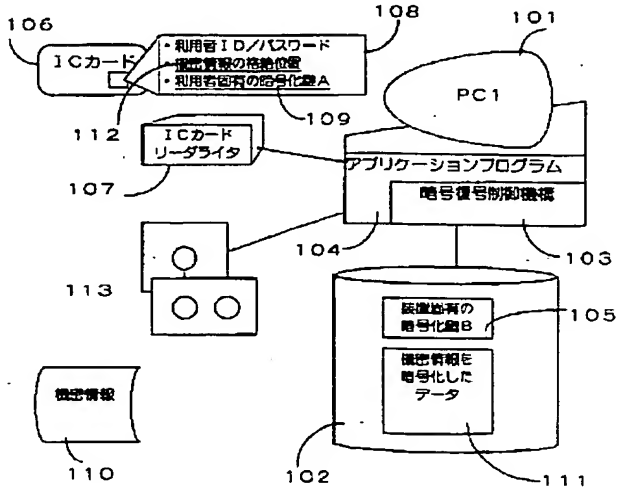
(54)【発明の名称】機密情報格納装置

(57)【要約】

【課題】格納された利用者の情報と利用者の入力情報を突き合わせて正しい時、機密情報にアクセスするための鍵を取出す方法などでは、利用者の情報と機密情報または機密情報にアクセスする鍵が同一の媒体に格納され悪意の第三者により媒体自体が盗まれた場合、総当たり的な方法で利用者の機密情報または機密情報にアクセスするための鍵を取出すことができる危険性がある。

【解決手段】本発明では機密情報を格納する時に利用者固有の鍵と装置固有の鍵とを使用することにより、暗号化し、より機密性の高い情報の格納方法を提供するものである。

図1



Ａを用い利用者情報が正しく入力された時のみ、鍵Ｂの復号化処理を行った出力ファイルを複写先の媒体に格納する機能を持たせる。複写先の媒体から別の装置のハードディスクに格納するには、媒体Ａを用いて利用者登録した後、媒体Ａと利用者の正当な入力があった時、初めて装置固有の鍵で暗号化してハードディスクに格納する機能により実現する。

【００１０】

【発明の実施の形態】以下本発明実施の具体的方法を示す。

【００１１】図１は本発明を適用する装置とその構成を示している。以下では携帯性に優れた比較的容量の小さい媒体をＩＣカード、装置本体に固定的に接続される外部記憶装置をハードディスクとして記述する。本発明において、暗号化制御機構１０３はコンピュータ装置１０１の外部記憶装置１０２にアプリケーションプログラム１０４に含まれて組み込まれる。例えばアプリケーションプログラムは電子証明書を必要とする電子商取引のクライアントなどが考えられ、機密情報は電子証明書などが想定できる。

【００１２】組み込みの際には、装置固有の鍵Ｂ１０５を作成し外部記憶装置１０２に格納する。装置固有の鍵Ｂ１０５の作り方は組み込まれた日付時刻やハードウエア固有のアドレス情報、あるいは乱数を用いて、他の装置と同一になる可能性が十分に小さいと判断できる方法で行う。

【００１３】次に利用者が暗号化制御機構１０３を起動し利用者の情報を登録する。このとき暗号化制御機構１０３はＩＣカードリーダライタ１０７により、初期化されたＩＣカード１０６内に利用者の情報１０８を書き込む。利用者の情報１０８の内容は利用者ＩＤ／パスワード、利用者固有の暗号化鍵Ａ１０９である。次に利用者が隠蔽しようとする機密情報１１０を指定する。

【００１４】これは多くの場合外部媒体１１２により読み込まれる。暗号化制御機構１０３は機密情報１１０を読取り利用者固有の鍵Ａ１０９により暗号化する。この結果、得られたファイルを更に装置固有の暗号鍵１０５により暗号化した結果得られたファイルを装置の外部記憶装置内の利用者が指定した位置に書き込む。利用者が指定した位置はＩＣカードの中に機密情報の格納位置１１２として書き込まれる。

【００１５】以下、それぞれの処理の詳細を説明する。図２にアプリケーションプログラム１０４のインストール処理のフローを示す。プログラムのインストールを開始すると通常のインストールと同様にプログラムの組込み２０１を行う。２０１には必要なディレクトリの作成、必要なプログラムファイル等の圧縮解凍および複写、プログラム動作用環境変数の設定、レジストリの設定等が含まれる。

【００１６】２０１が終了した後、装置固有の暗号鍵Ｂの生成２０２、鍵Ｂのハードディスクへの格納２０３を行いインストール処理を終了する。図３は利用者登録処理の流れを示している。まず利用者情報の読込み（利用者ＩＤ）３０１、利用者情報の読込み（パスワード）３０２を行う。これらは利用者による画面入力を読取る方法で実施する。

【００１７】次にＩＣカードを読取り３０３、データが既に存在する場合は初期化してよいかどうかを利用者に判断させる（３０４，３０７）。その後利用者固有の暗号鍵Ａを生成３０５し、利用者情報、暗号化鍵ＡをＩＣカードに書き込む。図４は機密情報の格納処理１を示す。機密情報格納処理１は全く機密情報が暗号化されていない状態から暗号化されハードディスクに格納されるまでの処理である。

【００１８】まず利用者情報、ＩＣカードの読込み（４０１，４０２）利用者の入力が正しいかを判定し４０３、正しければ機密情報の読込み４０４、ＩＣカードから暗号化鍵Ａを取出し４０５、暗号化鍵Ａで機密情報を暗号化４０６する。

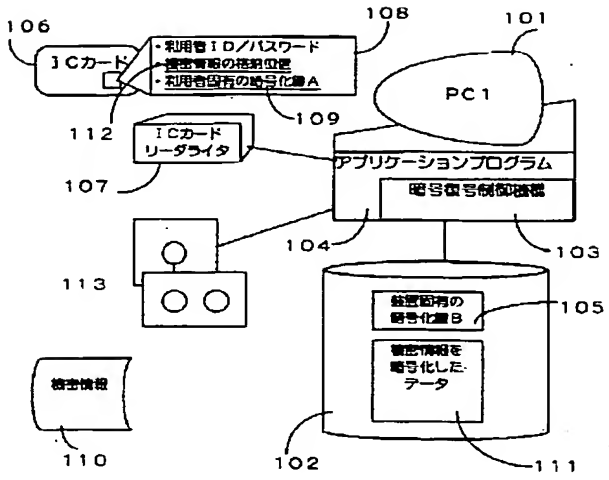
【００１９】次にハードディスクから装置固有の暗号化鍵Ｂを取出し、鍵Ａで暗号化された機密情報をさらに暗号化鍵Ｂで暗号化４０８する。最後に暗号化された機密情報の格納位置を利用者に問合わせ４０９、指定された格納位置情報をＩＣカードに書き込む４１０とともに暗号化した機密情報を指定された格納位置に格納４１１する。なお、利用者情報の入力が正しくなく規定回数を超えた誤入力があった場合は処理を中止する（４１２，４１３）。

【００２０】図５、図６は上記で格納された暗号化された機密情報を別の媒体に複写する処理の手順と同様の機能がインストールされた別の装置のハードディスクにに媒体を経由して機密情報を格納する方法を示す。図５の複写処理では、まず利用者情報の読込み５０１、ＩＣカードの読込み５０２を行い入力が正しかった場合５０３は、ＩＣカードから格納位置情報を読取り５０４、格納位置に格納された暗号化された機密情報を読込み５０５、暗号化鍵Ｂを取出し５０６、機密情報の暗号化鍵Ｂによる復号化５０７を行う。次に複写先の位置を利用者から画面入力させ５０８、鍵Ｂで複合された機密情報（鍵Ａで暗号化されている）を複写先に指定された媒体に格納５０９する。利用者情報の入力誤りは図４と同様（５１０，５１１）。

【００２１】図６の機密情報格納処理２（別の装置への格納処理）では、まず利用者情報の読込み６０１、ＩＣカードの読込み６０２、利用者の入力が正しかった場合６０３には、入力元ファイルの位置情報を利用者に入力させ６０４、暗号化鍵Ｂで復号化された機密情報（暗号化鍵Ａで暗号化されている）を入力元ファイルの位置から読込み６０５、暗号化鍵Ｂ’を取出し６０６（鍵Ｂ’：別の装置であるため鍵Ｂと異なることを意味す

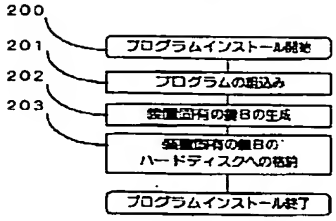
【図１】

図１



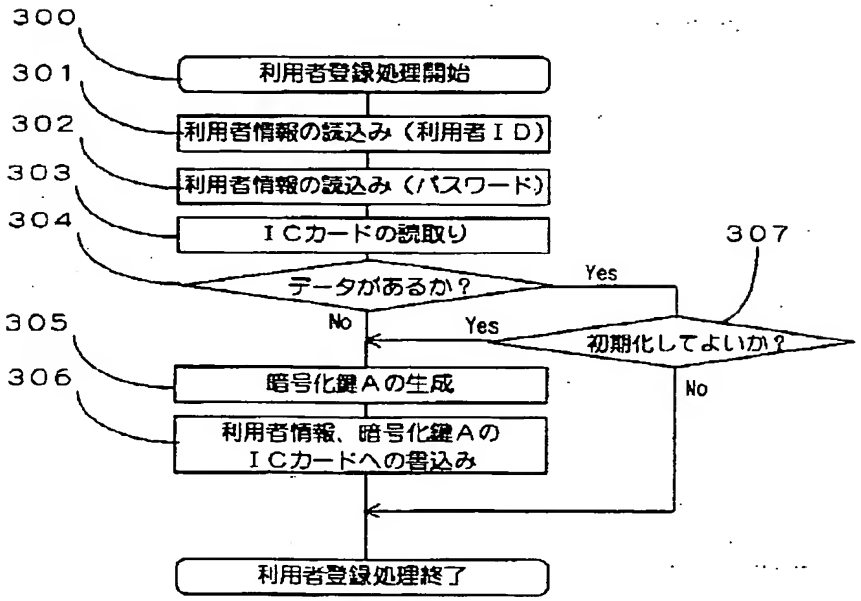
【図２】

図２



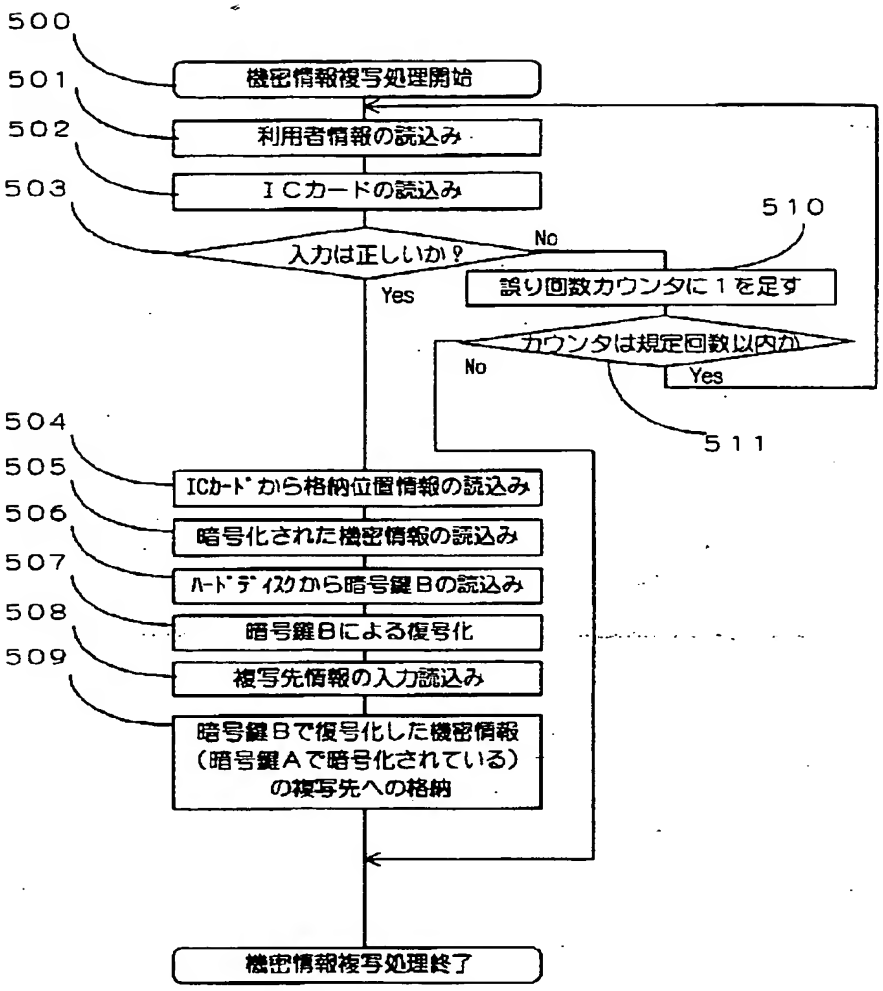
【図３】

図３



【図５】

図５


500
501
機密情報複写処理開始
502
利用者情報の読込み
503
ＩＣカードの読込み
入力は正しいか？
No
510
誤り回数カウンタに１を足す
Yes
カウンタは規定回数以内か
No
Yes
511
504
505
ICｶｰﾄﾞから格納位置情報の読込み
506
暗号化された機密情報の読込み
507
ﾊｰﾄﾞﾃﾞｨｽｸから暗号鍵Ｂの読込み
508
暗号鍵Ｂによる復号化
509
複写先情報の入力読込み
暗号鍵Ｂで復号化した機密情報
（暗号鍵Ａで暗号化されている）
の複写先への格納
機密情報複写処理終了